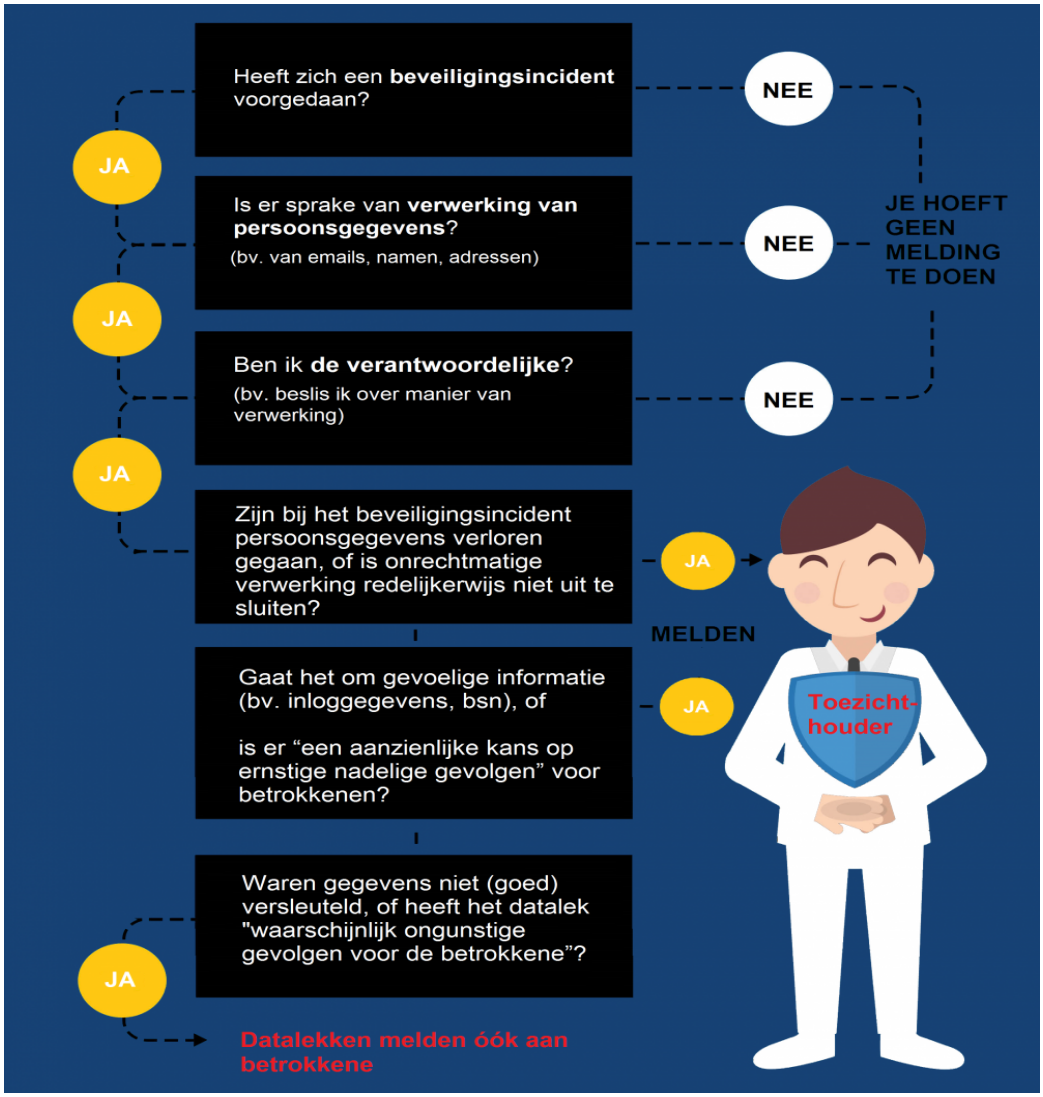
VESA NETWORK SOLUTIONS

Datanetwerken - ICT Beheer - Service - Onderhoud - Reparatie - Inspectie

Erkend Uneto VNI Installateur - Lid Vakgroep ICT - MVO Nederland Partner

Procedure Melding Datalekken

Handleiding voor het correct en tijdig afhandelen van datalekken



Inleiding
Sinds 1 januari 2016 is het wettelijk verplicht om datalekken te melden.

Zowel grootschalige inbraak als ieder kwijtraken of onbevoegd gebruik van persoonsgegevens telt als een datalek. Onder de AVG blijft dit ongewijzigd. Daarnaast zijn er consequenties verbonden aan het lekken van data. De AVG stelt boetes die kunnen oplopen tot 10 miljoen euro of 2% van de jaaromzet per overtreding.

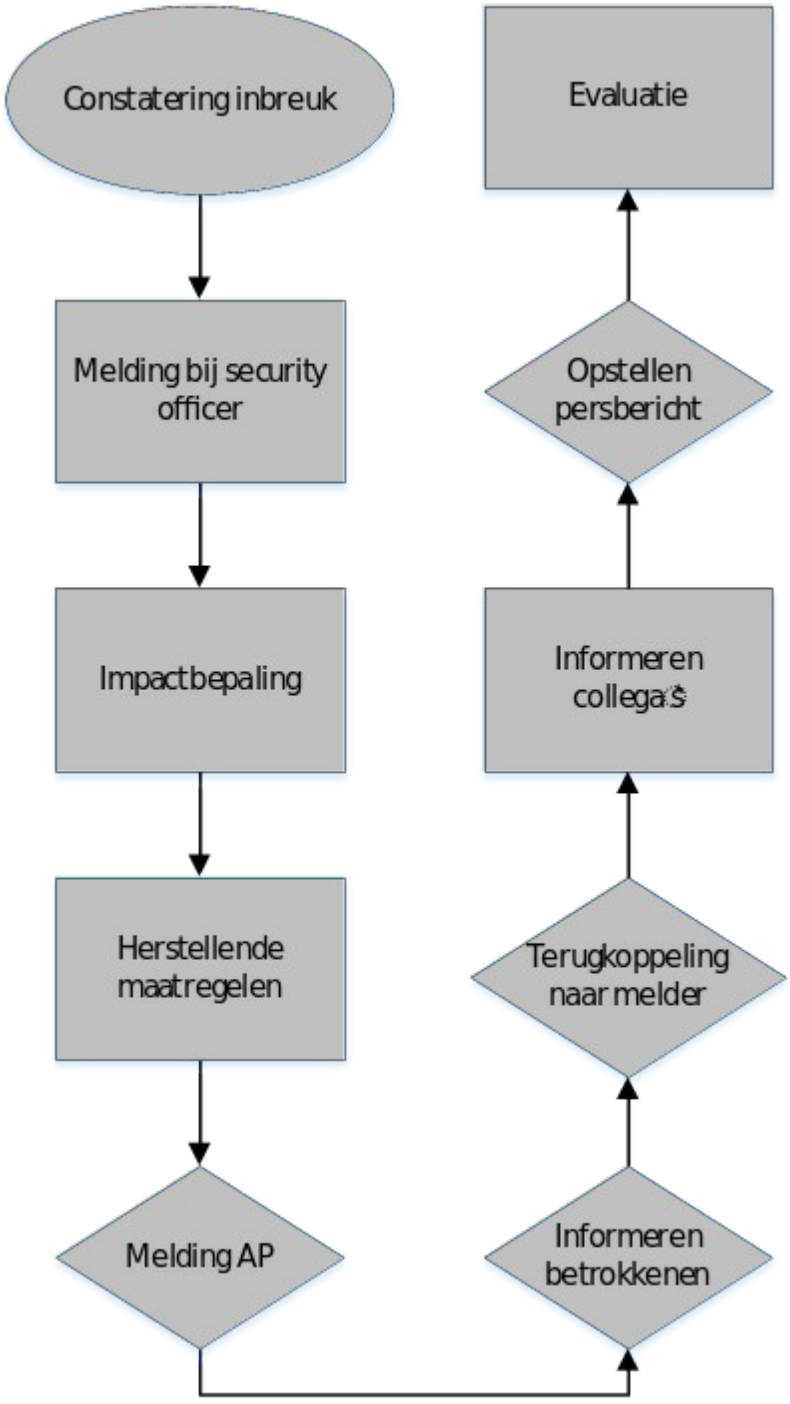
Er is sprake van een datalek wanneer persoonsgegevens verloren raken of een onrechtmatige verwerking van deze gegevens niet kan worden uitgesloten. Onder een onrechtmatige verwerking kan onder meer het aanpassen en veranderen van, of onbevoegde toegang tot persoonsgegevens worden verstaan. Het gaat om een brede definitie: er is niet alleen sprake van een datalek als een hacker toegang tot de persoonsgegevens krijgt.

Ook verlies van USB-sticks of een e-mail met de adressen in het CC-veld in plaats van het BCC-veld, telt als datalek.

Zoals hiervoor is beschreven moet het gaan om een lek waarbij persoonsgegevens zijn betrokken. Een persoonsgegeven is informatie over een natuurlijk persoon. Een hack waarbij gegevens over bedrijven of technische informatie wordt gestolen kan niet worden aangemerkt als datalek in de zin van de wet.

NB. De procedure geschreven voor een middelgroot bedrijf. Inventariseer of de procedure aansluit bij uw werkwijze. Pas de procedure waar nodig aan, maar onthoudt dat een melding bij de Autoriteit Persoonsgegevens binnen 72 uur moet plaatsvinden.

Algemene procedure



Algemeen stappenplan

TAKEN EN VERANTWOORDELIJKHEDEN[1]

Functie	Taken
Security Officer / Meldpunt	Eerste aanspreekpunt voor het melden van datalekken. Inventariseren de benodigde gegevens.
Privacy of security officer	Actiehouder procedure. Initieert en houdt zicht op alle te doorlopen stappen. Doet melding aan Autoriteit Persoonsgegevens.
Team datalekken	Bestaat bijvoorbeeld uit privacy / security officer, technisch manager, eventueel een jurist. Beslissen over uit te voeren acties.
Engineers	Onderzoeken het lek en treffen (i.s.m. technisch manager) de benodigde maatregelen. Onderhouden waar nodig contact met leveranciers.

ALGEMENE PROCEDURE

Let op: binnen 72 uur na ontdekking van het datalek moet de melding bij de Autoriteit Persoonsgegevens gedaan zijn, ongeacht het weekend of vrije dagen.

1) Constatering inbreuk op de beveiliging van de systemen door:
    a. Medewerker
        i. Direct melden bij de security officer. Als de security officer niet beschikbaar is, meldt de medewerker het bij zijn manager. De manager draagt vervolgens de verantwoordelijkheid om de security officer z.s.m. te informeren.
        ii. Inventarisatie van het datalek door de security officer in samenwerking met manager aan de hand van de geformuleerde vragen in *bijlage 1*.

    b. Klant
        i. Stuurt een e-mail of neemt telefonisch contact op.
        ii. Medewerkers zetten de informatie door naar de security officer. Bij telefonische melding zet de medewerker de call door naar de security officer [TELFOONNUMMER]. Als de security officer niet bereikbaar is, inventariseert de medewerker de informatie a.d.h.v. *bijlage 1* en zet deze in een e-mail naar de security officer en manager.

1Verdeel deze taken over de verschillende functies binnen uw bedrijf.

   c. Derde partij
      i. Stuurt een e-mail naar het algemene e-mailadres of belt het algemene nummer.
      ii. E-mail wordt doorgezet naar security officer. Bij een telefonische melding zet de medewerker de call door naar de security officer [TELFOONNUMMER]. Als de security officer niet bereikbaar is, inventariseert de medewerker de informatie a.d.h.v. *bijlage 1* en zet deze in een e-mail naar de security officer en manager.

2) Direct melden bij security officer. De security officer licht onmiddellijk het team datalekken en de directie in (**terstond**).
   Is de security officer niet op korte termijn beschikbaar dan licht de manager het team datalekken en de directie in (**terstond**).

3) Onderzoek naar de omvang en technische aspecten datalek door de technisch manager in samenwerking met engineers (**binnen 24 uur**).
   a. Welke inbreuk op de beveiligingsmaatregelen heeft plaatsgevonden en wanneer?
   b. Welk onderdeel van het IT-systeem is betrokken en/of welke apparatuur. Eventueel: waar is de apparatuur verloren/gestolen?
   c. Welke gegevens zijn (mogelijk) betrokken?
   d. Wat zijn de (verwachte) consequenties van het incident?

   Tegelijkertijd inwerkingtreding juridisch stappenplan door de security officer [en de jurist].

4) De engineers identificeren maatregelen om de beveiliging te herstellen en voeren deze uit na bespreking met het team datalekken (**binnen 72 uur na melding. Indien niet haalbaar, zo spoedig mogelijk**).

5) Als het incident moet worden gemeld of melding wenselijk is, stelt de security officer, in overleg met de directie, de jurist en eventueel de engineers, de melding naar de AP op (**binnen 72 uur**).[2]

6) Indien nodig: informeren betrokkenen (**tegelijkertijd met melding AP**).[3]

2Zie het ‘juridisch stappenplan’ op de pagina 7.
3Zie bijlage 2.

7) Indien nodig: terugkoppeling naar melder (**na melding AP**).

8) Informeren (relevante) medewerkers (**na melding AP**).

9) Indien nodig: directie stelt een persbericht op (**na melding AP**).

10) Evaluatie van de procedure met team datalekken. Initiatie door security officer.

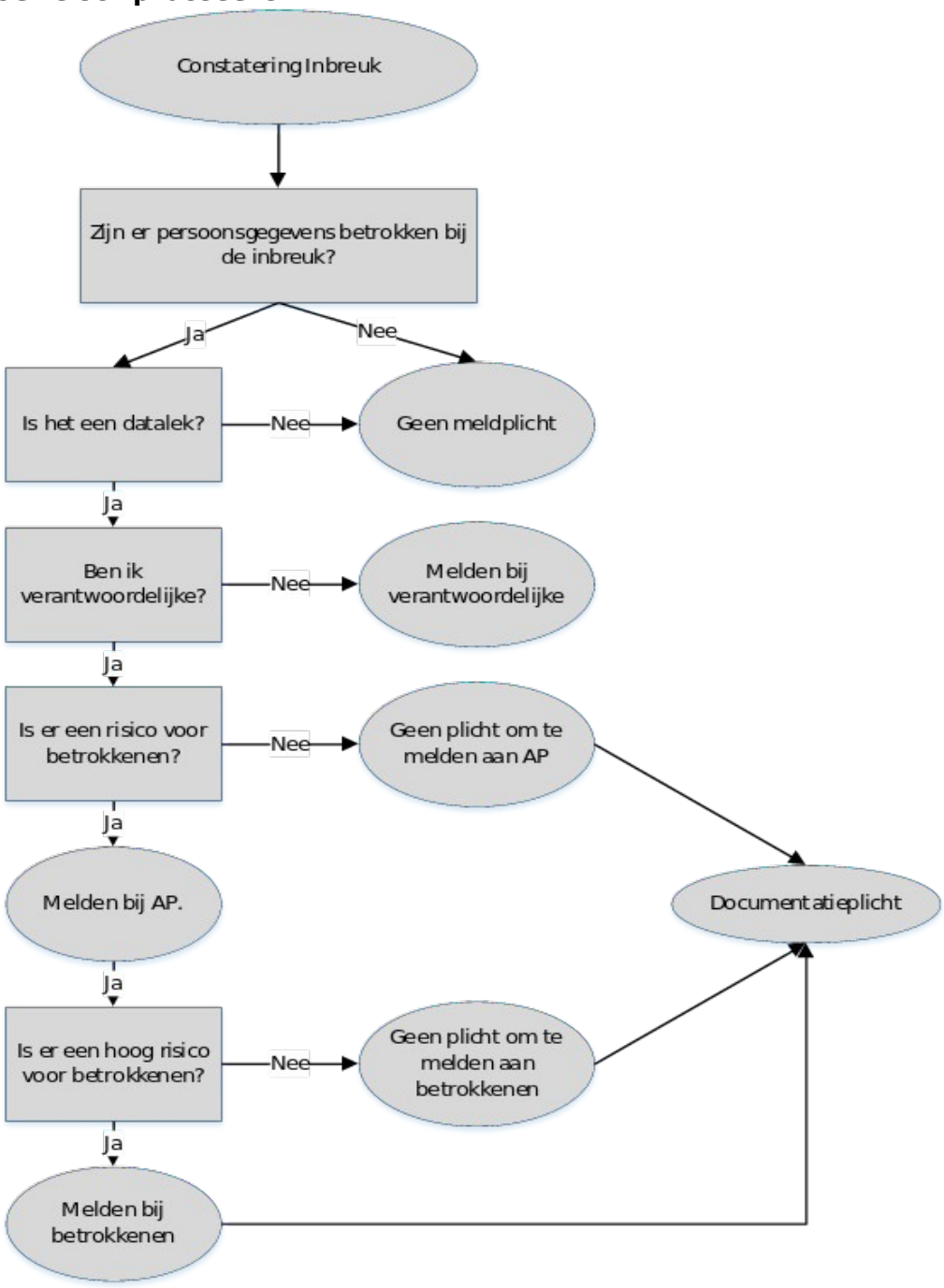
PROCEDURE BIJ CONSTATERING DATALEK TIJDENS HET WEEKEND/VRIJE DAGEN

1) Constatering of vermoeden van inbreuk op de beveiliging van de systemen door een medewerker, via een klant of derde partij.
    a. Persoon die het de constatering doet of binnen krijgt, licht de security officer in.
    b. Security officer treedt in overleg met de directie.
    c. Directie beslist of actie moet worden ondernomen.

2) Security officer schakelt wanneer nodig team datalekken in.

3) Verder vanaf stap 5 van bovenstaande procedure.

Juridisch procedure



Juridisch stappenplan

1) Constatering inbreuk op beveiliging systemen of verlies van apparatuur.

2) Welke gegevens waren toegankelijk?

3) Zijn deze gegevens aan te merken als persoonsgegevens?
    a. Persoonsgegevens zijn elke gegeven betreffende een geïdentificeerde of identificeerbare persoon. Een persoon is identificeerbaar als zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.

4) Is er sprake van een datalek?
    a. Zijn de verwerkte persoonsgegevens onherstelbaar verwijderd/aangetast of is er sprake van een onrechtmatige verwerking?
    Een onrechtmatige verwerking is het onbedoeld/onbevoegd wijzigen, verstrekken of toegankelijk maken van persoonsgegevens. Hanteer de volgende vuistregel: persoonsgegevens komen waar zij niet behoren te zijn.
    Zo ja, dan is er sprake van een datalek.

    b. Kan er redelijkerwijs worden uitgesloten dat er persoonsgegevens verloren zijn gegaan of onrechtmatige zijn verwerkt?[4]
    Zo ja, dan is er geen sprake van een datalek.

5) Is mijn bedrijf de verantwoordelijke voor de verwerking?
    a. Verantwoordelijke is degene die, alleen of tezamen met anderen, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.
    Voorbeeld: u heeft de salarisadministratie uitbesteed aan een extern bedrijf. Dit bedrijf heeft gegevens van uw personeel nodig om de salarisverwerking uit te voeren. In deze constructie bent u verantwoordelijke, omdat:
        a) u het doel stelt, namelijk de gegevens worden gebruikt ten behoeve van de salarisverwerking;

        b) u (gedeeltelijk) de middelen bepaalt. U heeft het bedrijf uitgekozen en geïnventariseerd welke systemen worden gebruikt, u heeft aangegeven hoe de gegevens wilt ontvangen, enz. Dat de andere partij ook gedeeltelijk zelf haar werkwijze bepaalt is geen bezwaar.

4Bijvoorbeeld wanneer de persoonsgegevens zijn beveiligd met sterke encryptie en het wachtwoord is niet uitgelekt.

b. Voor de gegevensverwerkingen die in samenwerking met Geen Draden Meer plaatsvinden bestaat een gedeelde verantwoordelijkheid. In dat geval kunt u contact opnemen met Geen Draden Meer om de verdere afhandeling af te stemmen.
c. Wanneer uw bedrijf niet is aan te merken als verantwoordelijke, bent u verplicht degene die de verantwoordelijke is op de hoogte te brengen van het datalek.

6) Moet dit lek gemeld worden aan de Autoriteit Persoonsgegevens?
   a. Een datalek moet worden gemeld bij de AP, tenzij het niet waarschijnlijk is dat de inbreuk een risico voor de betrokkenen inhoudt. Bijvoorbeeld wanneer:
      i. De persoonsgegevens publiekelijk beschikbaar zijn (openbare informatie);
      ii. De persoonsgegevens zijn versleuteld en het wachtwoord is niet uitgelekt;
      iii. Het gaat om onbedoeld verlies van persoonsgegevens, terwijl deze gegevens via een back-up zijn te herstellen.

   b. Een melding kan worden gedaan op de website van de AP (www.autoriteitpersoonsgegevens.nl).

7) Moet dit lek gemeld worden aan de betrokkene?
   a. Een datalek moet gemeld worden aan de betrokkene wanneer de inbreuk waarschijnlijk een hoog risico voor de betrokkene inhoudt.
   Van een hoog risico is sprake wanneer de verwachte nadelige gevolgen van het datalek zich met grote waarschijnlijkheid voordoen. Voorbeelden van nadelige gevolgen: identiteitsdiefstal, reputatieschade, financiële verliezen, ongewenste communicatie, enzovoorts.[5]

5Het criterium “waarschijnlijk een hoog risico” is een vaag begrip. De wetgever heeft dit begrip niet duidelijk afgebakend. De praktijk moet uitwijzen wat precies met dit criterium wordt bedoeld.

b. Bieden de technische beschermingsmaatregelen (zoals encryptie) die zijn genomen voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten?
    i. Zijn de persoonsgegevens onherstelbaar verwijderd of aangetast? Dan heeft encryptie geen zin en moeten betrokkenen worden ingelicht.
    ii. Waren alle persoonsgegevens versleuteld op het moment dat de inbreuk plaatsvond?
    iii. Is de versleuteling adequaat?
    iv. Is het restrisico acceptabel?

    Zo ja, geen melding aan betrokkenen verplicht.

c. Zijn er direct maatregelen genomen om ervoor te zorgen dat betrokkenen geen nadeel van het datalek ondervinden? Zo ja, geen melding aan betrokkenen verplicht.

d. Is het informeren van alle betrokkenen een onevenredige zware inspanning (bijvoorbeeld omdat het om een zeer groot aantal betrokkenen gaat)? In dat geval is een persoonlijke mededeling per betrokkene niet nodig en kunnen betrokkenen op een andere manier worden geïnformeerd.

8) Al hoeft een datalek niet aan de autoriteit of aan de betrokkene te worden gemeld, er geldt wel een registratieplicht. Alle datalekken die zich hebben voorgedaan moeten door de onderneming op een centrale plaats worden gedocumenteerd.

Bijlage 1 – inventarisatieplan datalekken

1) Naam, bedrijf, telefoonnummer en e-mailadres melder noteren.

2) Wanneer (datum en tijd) en hoe is het lek geconstateerd?

3) In welk systeem bevindt het lek zich?

4) Hoe kan het lek worden gebruikt?
    a. Zorg dat de werking van het lek duidelijk is. Het lek moet reproduceerbaar zijn.

5) Welke gegevens zijn toegankelijk?

6) Welke handelingen met betrekking tot de gegevens zijn mogelijk?
    a. Denk aan inzien, kopiëren, veranderen, verwijderen of vernietigen, enz.

7) Heeft de melder ideeën hoe het lek hersteld kan worden?

8) Gaat de melder het datalek publiekelijk maken? Zo ja, wanneer?
    a. Indien ja, verzoek de melder 72 uur te wachten zodat er eerst maatregelen kunnen worden getroffen.

Bijlage 2 – informeren betrokkenen

Sommige datalekken zijn zo ernstig dat de betrokkene(n) moet(en) worden ingelicht. Betrokkenen zijn de personen op wie de gelekte persoonsgegevens betrekking hebben. Wanneer de betrokkene precies moet worden geïnformeerd is hiervoor al beschreven. In deze bijlage wordt ingegaan op de vraag hoe de betrokkene moet worden geïnformeerd. In de kennisgeving wordt in ieder geval vermeld:

- De aard van de inbreuk (wat is er gebeurd?).
  Bij het beschrijven van de aard en inhoud van de inbreuk kan met een algemene omschrijving worden volstaan. Uitweiden over de technische details is niet nodig. Er moet aan bod komen welke persoonsgegevens zijn gelekt, wat hiervan de gevolgen voor de betrokkene kunnen zijn en welke maatregelen zijn genomen om de inbreuk aan te pakken. Belangrijk is dat beschrijving in duidelijke en eenvoudige taal is.

- De vermoedelijke datum en tijdstip van het incident.

- De ernst van het datalek.
  Informeer de betrokkene over de gevolgen die zich waarschijnlijk kunnen voordoen naar aanleiding van het datalek. Denk aan identiteitsdiefstal, reputatieschade, financiële verliezen, ongewenste communicatie, enz.

- De maatregelen die zijn genomen om de inbreuk aan te pakken en de nadelige gevolgen voor betrokkenen te beperken. Hoe is het beveiligingslek gedicht? Is een procedure aangescherpt? Kan de betrokkene bijv. een schadeclaim indienen?

- De maatregelen die de betrokkene moet nemen om de negatieve gevolgen van de inbreuk te beperken. Denk hierbij aan het veranderen van gebruikersnamen en wachtwoorden.

- Contactgegevens/een centraal informatiepunt.
  Op deze manier kan de betrokkene u bereiken als hij of zij nog vragen heeft over het datalek. De instanties waar de betrokkene meer informatie over de inbreuk kan krijgen. Indien van toepassing.

Het belangrijkste is dat zo veel mogelijk betrokkenen worden bereikt met de informatie om de nadelige gevolgen te beperken. De mededeling is vormvrij en mag dus schriftelijk maar ook elektronisch worden gedaan.